

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



(19)

(11) Publication number:

11024916 A

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: 09181182

(51) Intl. G06F 9/06 G06F 15/00 G09C 1/00 H04L
Cl.: 9/32

(22) Application date: 07.07.97

(30) Priority:

(43) Date of application publication: 29.01.99

(84) Designated contracting states:

(71)

Applicant: FUJI XEROX CO LTD

(72) Inventor: KOJIMA SHUNICHI
NAKAGAKI JUHEI
KONO KENJI

(74)

Representative:

(54) DEVICE AND METHOD
FOR MANAGING
SOFTWARE LICENCE

(57) Abstract:

PROBLEM TO BE SOLVED: To control soft ware and to manage a license offline.

SOLUTION: User specific information dU is taken out form a user information data base 310 based on the request of a user and a secret key D is obtained from a software information data base 320. A license ticket (t) is generated by $t=D-F(dU, n)$ and it is issued to the user. A function F is preferably a one-way hash function. The user can verify an access qualification to software by using the license ticket and user specific information to make use of the software. An item of the pertinent user of the user information data base 310 and an item of the pertinent user of the user information data base 320 are updated in accordance with issuance of the license ticket. Charging is executed based on the content of the software information data base 320 at an appropriate period.

ライセンスチケット発行装置 30

ライセンスチケット生成手段
301

ユーザ情報管理手段 302

ユーザ情報データベース
310

ソフトウェア情報管理手段 303

ソフトウェア情報データ
ベース 320

ライセンス数管理手段 304

ライセンスチケット
201

COPYRIGHT: (C)1999,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-24916

(43) 公開日 平成11年(1999) 1月29日

(51) Int. Cl.⁶

G 0 6 F 9/06

識別記号

5 5 0

F I

G 0 6 F 9/06

5 5 0 C

5 5 0 G

5 5 0 Z

15/00

3 3 0

15/00

3 3 0 E

G 0 9 C 1/00

6 4 0

G 0 9 C 1/00

6 4 0 B

審査請求 未請求 請求項の数15 O L (全 13 頁) 最終頁に続く

(21) 出願番号

特願平9-181182

(22) 出願日

平成9年(1997) 7月7日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 小島 俊一

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(72) 発明者 中垣 寿平

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(72) 発明者 河野 健二

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

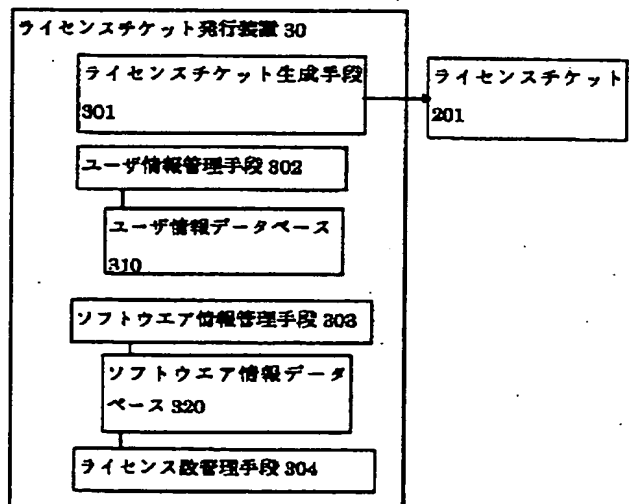
(74) 代理人 弁理士 澤田 俊夫

(54) 【発明の名称】 ソフトウェアライセンス管理装置および方法

(57) 【要約】

【課題】 オフラインでもソフトウェアの実行制御を行えるようにし、あわせてライセンスの管理を行えるようにする。

【解決手段】 ユーザの要求に基づいて、ユーザ情報データベース310からユーザ固有情報dUを取り出し、ソフトウェア情報データベース320から秘密鍵Dを得る。ライセンスチケットtは $t = D - F(dU, n)$ により生成され、ユーザに発行される。ユーザは、ライセンスチケットおよびユーザ固有情報を用いてソフトウェアのアクセス資格を証明でき、ソフトウェアを利用できる。ライセンスチケットの発行に応じて、ユーザ情報データベース310の該当ユーザの項目とソフトウェア情報データベース320の該当ソフトウェアの項目が共に更新される。適当な時期で、このソフトウェア情報データベース320の内容に基づき課金が行われる。



【特許請求の範囲】

【請求項1】 証明データ生成装置と、証明データ検証装置とを有し、

前記証明データ生成装置は、

認証用データを記憶する第1の記憶手段と、

ユーザの固有情報を記憶する第2の記憶手段と、前記ユーザの固有情報とアクセス資格認証の特徴情報とに対し、

所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と、

前記第1の記憶手段に保持されている認証用データと、

前記第2の記憶手段に記憶されている前記ユーザの固有情報と、前記第3の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを具備し、

上記証明データ検証装置は、

利用を制限されたソフトウェアを記憶するソフトウェア記憶手段と、

認証用データを記憶する第4の記憶手段と、

証明データを記憶する第5の記憶手段と、

前記第5の記憶手段に記憶されている前記証明データが、前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段と、

前記証明データ検証手段による検証が成功した時のみ、前記ソフトウェア記憶手段に記憶されている前記ソフトウェアの利用を可能にする実行制御手段とを具備し、

前記証明データ検証装置と、前記証明データ生成装置とが、互いに通信してユーザのアクセス資格認証をおこない、正当な前記証明用補助情報を有するユーザのみにソフトウェアの利用を可能にすることを特徴とするソフトウェアライセンス管理装置。

【請求項2】 前記ユーザ向けに前記証明用補助情報を発行する証明用補助情報発行装置をもち、発行の記録に基づいてソフトウェアの管理をおこなうことを特徴とする請求項1に記載のソフトウェアライセンス管理装置。

【請求項3】 前記ユーザ向けに前記証明用補助情報を発行する証明用補助情報発行装置を持ち、前記証明用補助情報を発行した数に基づいて、許諾したソフトウェアのライセンス数を管理することを特徴とする請求項1に記載のソフトウェアライセンス管理装置。

【請求項4】 前記証明用補助情報発行装置は、さらに前記証明用補助情報を発行可能な上限数を記憶する発行上限記憶手段と、既に発行し、かつ有効な証明用補助情報の数を記憶する第6の記憶手段と、前記第6の記憶手段に記憶されている有効ライセンス数が、前記発行上限記憶手段に記憶した上限数に達すると、それ以上の証明用補助情報の発行を行わないライセンス数管理手段をもつことを特徴とする請求項2または3に記載のソフトウェアライセンス管理装置。

【請求項5】 前記証明データ生成装置において、利用制御情報を記憶する利用制御情報記憶手段をさらに備

え、前記証明データ生成手段は、前記第1の記憶手段に保持されている認証用データと、前記第2の記憶手段に記憶されている前記ユーザの固有情報と、前記第3の記憶手段に記憶されている前記証明用補助情報と、前記利用制御情報記憶手段に記憶されている前記利用制御情報とに所定の計算を施して証明データを生成し、前記ユーザの固有情報と、前記アクセス資格認証の特徴情報と、前記利用制御情報とに対し、所定の計算を実行した実行結果である証明用補助情報を有するユーザのみに前記ソフトウェアの利用を可能にすることを特徴とする請求項1、2、3または4に記載のソフトウェアライセンス管理装置。

【請求項6】 前記利用制御情報は、前記証明用補助情報の有効期間を示すデータを含むことを特徴とする請求項5に記載のソフトウェアライセンス管理装置。

【請求項7】 既に発行した前記利用制御情報の有効期間情報により、前記第6の記憶手段に記憶されている有効ライセンス数の更新をおこなうライセンス数管理手段をもつことを特徴とする請求項1、2、3、4、5または6に記載のソフトウェアライセンス管理装置。

【請求項8】 前記利用を制限されたソフトウェアは、少なくとも一部分を暗号化した状態で前記ソフトウェア記憶手段に記憶され、前記アクセス資格認証の特徴情報が暗号化関数における第1の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第2の復号鍵を前記第1の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ生成手段によって生成された証明データが前記第2の復号鍵であり、前記第2の復号鍵を用いて前記暗号化されたプログラムの一部分を復号して、前記プログラムの実行をおこなうことを特徴とする請求項1、2、3、4、5、6または7に記載のソフトウェアライセンス管理装置。

【請求項9】 少なくとも、前記第2の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項1、2、3、4、5、6、7または8に記載のソフトウェアライセンス管理装置。

【請求項10】 少なくとも、前記第2の記憶手段と、前記証明データ生成手段とが、ICカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項1、2、3、4、5、6、7または8に記載のソフトウェアライセンス管理装置。

【請求項11】 前記利用を制限されたソフトウェアをもつ前記証明データ検証装置をCD-ROMやDVD-ROMなどの媒体に格納して流通可能にしたことを特徴とする請求項1から10に記載のソフトウェアライセンス管理装置。

【請求項12】 前記利用を制限されたソフトウェアをもつ前記証明データ検証装置をWWWサーバやFTPサ

サーバなど、ネットワーク上のサーバのサービスとして流通可能にしたことを特徴とする請求項 1、2、3、4、5、6、7、8、9 または 10 に記載のソフトウェアライセンス管理装置。

【請求項 13】 少なくともユーザの固有情報とソフトウェアのアクセス資格認証の特徴情報とに基づいて認証用補助情報を発行する手段と、前記証明用補助情報を発行した数に基づいて、許諾したソフトウェアのライセンス数を管理する手段とを有することを特徴とするソフトウェアライセンス管理用の認証用補助情報発行装置。

【請求項 14】 前記証明用補助情報の発行可能な上限数を記憶する発行上限記憶手段と、既に発行し、かつ有効な証明用補助情報の数を記憶する有効ライセンス数記憶手段とをさらに有し、前記ライセンス記憶手段に記憶されている有効ライセンス数が、前記発行上限記憶手段に記憶した上限数に達すると、それ以上の証明用補助情報の発行を行わないようにすることを特徴とする請求項 13 に記載のソフトウェアライセンス管理用の認証用補助情報発行装置。

【請求項 15】 認証用データを記憶する第 1 の記憶ステップと、ユーザの固有情報を記憶する第 2 の記憶ステップと、前記ユーザの固有情報とアクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第 3 の記憶ステップと、前記第 1 の記憶ステップによって保持されている認証用データと、前記第 2 の記憶ステップによって記憶されている前記ユーザの固有情報と、前記第 3 の記憶ステップによって記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成するステップと、利用を制限されたソフトウェアを記憶するステップと、認証用データを記憶する第 4 の記憶ステップと、証明データを記憶する第 5 の記憶ステップと、前記第 5 の記憶ステップによって記憶されている前記証明データが、前記アクセス資格認証の特徴情報に基づいて生成されていることを検証するステップと、前記検証が成功した時のみ、前記ソフトウェアの利用を可能にするステップとを有することを特徴とするソフトウェアライセンス管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ソフトウェアのライセンスを管理する方法とその装置に関する。

【0002】

【従来の技術】 従来、ソフトウェアは、フロッピーディスク等の物理媒体に格納され、物理媒体として売買されてきた。しかし、ソフトウェアのようなデジタル著作物は、オリジナルと寸分違わぬコピーを容易に作成することが可能であるという特質を持つために、簡単に不正

コピーされて使われることが多かった。近年、磁気ディスクなどコンピュータの記憶容量が大容量化されるにつれて、この不正コピーの数は増大しているといわれている。

【0003】 ソフトウェアは、ソフトウェアのプロバイダーとユーザとの間で、ライセンス契約（使用許諾契約）を結んで使用することが多いが、上述したようにソフトウェアは容易にコピーが可能であるため、ライセンス契約を行わずに不正コピーしたソフトウェアを利用するユーザも多い。

【0004】 また、企業や大学においても、社員や学生が企業内や大学内のコンピュータに勝手にソフトウェアを不正コピーして使用しているかどうかを把握する術がないため、知らぬ間に大量の不正コピーが行われていて、時に摘発されて、信用の失墜と膨大な賠償を被ることにもなりかねない。

【0005】 このような状況に対して、近年ライセンス管理システムと呼ばれるものが開発されてきている。ライセンス管理システムは、ライセンスを許可されていないユーザには、ソフトウェアの利用ができないように構成されたものであり、ソフトウェアを暗号化して配布したり、パスワードによる実行制御によって、利用制限をおこなっている。

【0006】 しかし、パスワードを他人に教えたり、暗号鍵ごとコピーして使ったりすることにより、結局は不正コピーと変わらない状況になってしまう。

【0007】 そこで、一つの解決方法として、米国 Sassafras 社の Key Server（商標）に代表されるような、ネットワーク上のライセンス管理サーバによって実行可能数を管理する方法が考えられている。この管理手法では、オリジナルのソフトウェアを暗号化などの方法で利用を制限し、それを公開する。オリジナルのソフトウェアは別に管理者しかアクセスできないところに物理的に鍵を掛けて保存する。ユーザはソフトウェア実行時にライセンスサーバからライセンス（鍵）の供与を受け、実行制御を解除し利用している。オンラインで発行されたライセンス（鍵）がなければソフトウェアは実行することができず、発行された鍵はユーザには見えないようにすることで不正使用を防止している。

【0008】

【発明が解決しようとする課題】 しかし、このようなネットワーク上のライセンスサーバによる管理方式では、オフライン時での使用制限をおこなうことが不可能である。ネットワークにアクセスし難いモバイル環境でも、正当なライセンスをもつ場合は正当にソフトウェアを実行出来ることが必要である。つまり、ユーザにオンライン・オフライン両方の環境下で、同じように実行制御が可能で、かつ不正な二次コピーの配布を防止出来る仕組みにすることが必要である。本発明は、上記従来の課題を解決し、オフラインでも実行制御ができるソフトウェ

ライセンス管理装置を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明によれば、上記目的を達成するに、所定の手法たとえば暗号化によってその利用を制限したソフトウェアに対して、ユーザのアクセス資格を認証する証明データ検証手段を設ける。他方、ユーザ側には、そのソフトウェアを利用できることを示す証明データ生成手段を設け、証明データ検証手段と証明データ生成手段とが相互に通信してユーザのアクセス資格を検証する。さらに、ソフトウェア側に、以上の検証結果が成功したときのみソフトウェアの復号等を行いプログラムを実行できるようにする実行制御手段を設ける。また、証明データを生成する際にはユーザの固有情報と証明用補助情報とが必要であり、所定の発行装置が、ユーザの固有情報とソフトウェアのライセンス情報に基づいて証明用補助情報を発行する。

【0010】この構成においては、ユーザはユーザの固有情報に対応する真正な証明補助情報を有していなければプログラムを実行させることができない。そしてこの証明補助情報を発行する装置が、証明補助情報の発行管理を通じてソフトウェアライセンスを管理することができる。

【0011】

【発明の実施の態様】以下、本発明の実施例について説明する。

【全体の構成】図1は、本発明の一実施例の構成を全体として示している。図1において、証明データ検証装置10はソフトウェアプロバイダにより提供される。この証明データ検証装置10は、利用を制限されたソフトウェア100を含み、さらに証明データ検証手段110と実行制御手段120とを有している。証明データ検証手段110は認証用データ111を生成し、証明データ生成装置20が管理する証明データ生成手段200に送る。ここでの通信手段は特に問わない、プロセス間の通信であってもネットワークを介した通信でも構わない。証明データ生成手段200は受け取った認証用データ111とその証明データを生成するのに必要なライセンスチケット201とユーザ固有情報202とから証明データ203を生成し、証明データ検証手段110に送る。証明データ検証手段110は、証明データ生成手段200から生成された証明データ203を受け取り、検証をおこなう。検証結果によって、実行制御手段120で利用制限を解除しソフトウェア100を利用できるようにする。

【0012】ユーザは証明データ生成に先立ち、ライセンスチケット201をライセンスチケット発行装置30から発行してもらう。ライセンスチケット発行装置30はライセンスチケットをユーザの固有情報202とアクセス資格認証の特徴情報300とから生成する。

【0013】なお、この実施例においては、図2に示す

ように、有効期限等の利用制限情報204を用いて利用を制限するようにしてもよい。図2において、図1と対応する箇所には対応する符号を付して詳細な説明を省略する。また、図1および図2において、証明データ生成装置20中において点線で囲んだ部分は耐タンパー装置で防御されている部分を部分を示す。

【0014】【アクセス資格認証の概略】以下に本実施例を詳細に説明する。まず、アクセス資格の認証について説明する。ユーザのアクセス資格の認証には、暗号化の手法が使用されるが、この例においてはRSA (Rivest-Shamir-Adelman) 公開鍵暗号系を用いる。もちろん、他の種々の暗号を用いることができる。

【0015】まず、ソフトウェアに対して認証用の公開鍵暗号鍵ペアとして公開鍵Eと秘密鍵Dとそれに対する法数nとを設定する。法数nはソフトウェアに対して設定する。ライセンス資格認証の特徴情報300としてこの秘密鍵Dを使用する。

【0016】この実施例では、以下の情報または計算を用いてライセンス資格の認証を行う。

①共通鍵暗号の鍵K：プログラムの少なくとも一部を暗号化して利用制限する。

②ユーザ固有情報dU

③ライセンス資格認証の特徴情報D

④ライセンスチケット $t = D - F(dU, n)$ または $D - F(dU, n, L)$

ただし、F() は好ましくは一方向ハッシュ関数である。Lは有効期限等の利用制限情報である。

⑤認証用データ $C = r^E K^E \pmod{n}$

ただし、rは乱数である。

⑥証明データ生成式： $C^t C^{r(dU, n, L)}$ または $C^t C^{r(dU, n, L)}$ \pmod{n}

⑦検証手法：乱数効果を除去して鍵Kを復元し、暗号化プログラムを復号する。

【0017】証明データ検証装置10と証明データ生成装置11とは相互にデータを通信して認証を行い、認証が成功するとソフトウェアを利用することが可能となる。認証は、まず、ソフトウェア利用の要求に応じて、証明データ検証装置10が認証用データ(Cまたは $C = r^E K^E$) 111を証明データ生成装置11に送出し、証明データ生成装置11は、この認証用データ111とユーザ固有情報(dU) 202とライセンスチケット($t = D - F(dU, n)$) 201とに対して所定の演算を実行して証明データ203を生成し、証明データ検証装置10に返す。ライセンスチケット(t)と、ユーザ固有情報(dU)と、認証の特徴情報(D, n)が対応していれば、証明データは、 $(rK)^D \pmod{n}$ となり、 $DE \pmod{n} = 1$ から、rKとなる。そして、乱数rを用いてKを算出する。この共通暗号鍵Kを用いて暗号化されているソフトウェアを復号して実行する。

【0018】[ソフトウェアの利用制限手法] つぎに、ソフトウェアの利用制限について説明する。この実施例では、ソフトウェアの利用制限の手法としては、共通鍵暗号系による暗号化を採用する。利用制限されたソフトウェア100(図1、図2)は図3に示すように予め処理されて、頒布される。図3において、まず、ソフトウェアの少なくとも一部を共通鍵暗号の鍵Kで暗号化する(S10)。つぎに鍵KをRSA暗号の公開鍵Eで暗号化し($S11$ 、 $K' = K^E \bmod n$)、暗号化した鍵K'を証明データ検証手段110が取り出せる状態でソフトウェアに埋め込む(S12)。

【0019】[認証用データ] つぎに認証用データ111の一例を説明する。認証用データ111は、この例では、 $C = r^E K' \bmod n$ である。ただし、rは乱数である。認証用データは、図4に示すように生成される。まず、暗号化された秘密鍵データK'を取り出す(S21)。つぎに乱数rを設定し、乱数rは保持しておく(S22)。そして $C = r^E K' \bmod n$ を計算し、Cの値とnとの組みを認証用データ111とする。ここで、乱数rは毎回変化し予測不可能なので、同じ証明データを再度使用できないようにする。したがってリプレイアタックに対処できる。

【0020】[ライセンス管理手法—ライセンスチケット発行] つぎに、ソフトウェアのライセンス管理の例を説明する。この例においては、ユーザが使用するソフトウェアに対するライセンスチケットの発行枚数に応じて、各ソフトウェアのプロバイダにライセンスフィーを支払うようになっている。

【0021】図5は、この管理例で用いるライセンスチケット発行装置30の構成をしめす。このライセンスチケット発行装置30は、ユーザの要求により、ユーザの証明データ生成に必要なライセンスチケット(t)201を生成し発行する装置である。

【0022】図5において、ライセンスチケット発行装置30は、ライセンスチケット生成手段301、ユーザ情報管理手段302、ユーザ情報データベース310、ソフトウェア情報管理手段303、ソフトウェア情報データベース320およびライセンス数管理手段304を含んで構成されている。

【0023】なお、先に説明したユーザ固有情報202とライセンス資格認証の特徴情報300としてのソフトウェアの秘密鍵Dとは、安全に秘密情報として管理されていなくてはならない。ユーザ固有情報(dU)202はユーザUに対する秘密情報でユーザ情報データベース310に安全に保存されている。ユーザへは証明データ生成手段200(図1)の一部として、安全な保護容器(例えばICカード)の中に保持されて渡される。この手順に関係する構成は本発明では限定しない。たとえば、別の第三者がこの配布をおこなってもよいし、ライセンスチケット発行装置30がこの機能を兼ねてい

かまわない。ユーザデータベース310へのアクセスはユーザ情報管理手段302によっておこなわれる。

【0024】図6はユーザ情報データベース310の構成例を示す。図6に示すように、ユーザ情報データベース310では、ユーザの識別子としてユーザIDをもち、ユーザ名U、ユーザ固有情報dU、発行したライセンスチケットの履歴をリスト形式で持っている。ユーザ情報データベース310を参照することにより、ユーザごとの発行したライセンス枚数や発行の履歴を調べることができる。

【0025】ソフトウェアに関する秘密鍵D(資格認証の特徴情報300)はライセンスチケット発行装置30が生成して、公開鍵Eをソフトウェアプロバイダに配布するか、または逆にソフトウェアプロバイダから秘密鍵Dを安全な手段で受け取り管理する方法が考えられる。このソフトウェアに対する公開鍵秘密鍵のペアの生成に関する構成は本発明では限定しない。秘密鍵Dはソフトウェア情報データベース320で安全に保持され、ソフトウェア情報管理手段303によって管理される。

【0026】図7は、ソフトウェア情報データベース320の構成例を示す。図7に示すように、ソフトウェア情報データベース320では、ソフトウェアのIDや名称、RSA法数n、秘密情報Dの他に、ライセンスチケットの発行枚数、必要ならばそのリストを保持することにする。ソフトウェア情報データベース320によって、そのソフトウェアに対して何枚のライセンスチケットが発行されているかを確認できることとなる。

【0027】図8は、ライセンスチケットの生成方法とそれに伴うデータベース310、320への操作を示す。図8において、まず、ユーザの要求により、発行するライセンスチケットのユーザUとソフトウェアnの情報を得る。すなわち、ユーザ情報データベース310からユーザ固有情報dUを取り出し(S30)、ソフトウェア情報データベース320から秘密鍵Dを得る(S31)。ライセンスチケットtはつぎの生成式により生成される(S32)。

【0028】

【数1】 $t = D - F(dU, n)$

ここでの関数F()は、上述のとおり、好ましくはは一方方向性ハッシュ関数である。関数の引数の各項は、単純な接合が考えられる。が本発明ではこれに限らない。すべての項目が関数の結果に影響するようなものであればどのような方式でもかまわない。

【0029】最後にユーザ情報データベース310の該当ユーザの項目とソフトウェア情報データベース320の該当ソフトウェアの項目を共に更新する(S33)。

【0030】適当な時期で、このソフトウェア情報データベース320の内容を調べて、各ソフトウェアに対するライセンスチケットの発行枚数によりソフトウェアプロバイダへライセンスフィーを支払う。

【0031】[他のライセンス管理手法] つぎに、ソフトウェアのライセンス管理の別の例を説明する。このライセンス管理の方法は、予め各ソフトウェアにはライセンス数の上限が設定されており、ライセンスチケットの枚数がその上限を超えては発行できないようにするものである。さらに、ライセンスチケットには有効期限を設ける。これにより、ライセンスチケットの失効の時間がくればソフトウェアは利用できなくなるので、新たな発行が可能になる。

【0032】図9は、この管理手法に用いるソフトウェア情報データベース320の構成例を示す。図9に示すように、このソフトウェア情報データベース320では、ソフトウェアのIDや名称、ソフトウェアにユニークなRSA法数 n 、秘密情報 D の他に、予め設定されたライセンス数、現在の有効ライセンスチケット数と、必要ならばそのリストを保持することにする。このソフトウェア情報データベース320によって、そのソフトウェアに対して同時に設定されたライセンス数(上限)までのライセンスチケットが発行することができる。

【0033】図10は、この管理手法にしたがうライセンスチケットの生成方法とそれに伴うデータベース310、320への操作を示す。図10において、まず、ユーザの要求により、発行するライセンスチケットのユーザ U とソフトウェア n の情報を得る。すなわち、ユーザ情報データベース310からユーザ固有情報 dU を取り出し(S40)、ソフトウェア情報データベース320から現在のライセンスチケット数が設定された上限を超えないかを調べて、現在のライセンスチケットの発行の可否を決める(S41、S42、S43)。発行が可能ならば、ソフトウェア情報データベース320から秘密鍵 D を取り出す(S46)。発行が不可能であれば、その旨をユーザに通知する(S45)。

【0034】ライセンスチケットには利用制限情報 L を付属させることができる(S47)。これにより、例えば、ライセンスに有効期間を設定し、この結果、有効期間を過ぎた場合(または、有効期間前)使用することができないライセンスチケットを作成することができる。この場合、ライセンスチケット t はつぎの生成式で生成されて発行される(S48)。

【0035】

【数2】 $t = D - F(dU, n, L)$

ここでの関数 $F()$ は、上述のとおり、好ましくは一方方向性ハッシュ関数である。関数の引数の各項は、単純な接合が考えられるが、本発明ではこれに限らない。すべての項目が関数の結果に影響するようなものであればどのような方式でもかまわない。

【0036】最後にユーザ情報データベース310の該当ユーザの項目とソフトウェア情報データベース320の該当ソフトウェアの項目を共に更新する(S49)。

【0037】このライセンス管理方式では、予め設定し

たライセンス数を超えてのユーザへの使用は不可能なので、ソフトウェアプロバイダへはその数のライセンスフィーを支払う。

【0038】[証明データ生成] 図11は、証明データ203の生成方法の一例を示す。ここでは図9を参照して説明した管理手法に即して説明する。図11において、まず、証明データ検証装置10から認証用データ (C, n) を受け取る(S50)。つぎに受け取った認証用データ (C, n) の n の値に基づいて、ソフトウェア情報データベース320を参照して、対応するライセンスチケット (t) 201と利用制限情報 L を取得する(S51)。このライセンスチケット201は、前述の方法でライセンスチケット発行装置30より発行される。次に、ライセンスチケットの利用制限情報をチェックする(S52)。例えば利用制限情報が有効期間であれば、現在時刻と比較する。利用が許容される場合には、つぎの式にしたがって証明データ R を生成する(S53)。

【0039】

【数3】 $R = C^t C^{F(dU, n, L)}$

利用制限情報 L と $t = D - F(dU, n, L)$ とは組で構成され、 L の中に有効期間などの制限情報を織り込まれている。ユーザは L の偽造をおこなっても、対応するライセンスチケット t の偽造は不可能なので、ライセンスチケットの完全性は保たれている。

【0040】また、証明データの計算に必要なユーザ固有情報 dU は安全に保持・実行されなければならないので、ユーザ固有情報を保持する部分、および証明データの計算を計算する部分を、一般にはICカードのような外部からの観測を困難にするような小型演算装置を持ったデバイスで実装することが要望される。

【0041】[証明データ検証] 図12は、証明データ203の検証と、そこから得られた K による実行制御手段120によるソフトウェアの復号化の一例を示す。図12において、まず、証明データ検証装置10は証明データ生成装置20から証明データ R を受け取る(S60)。証明データ検証手段110は、受け取った証明データ R 203をソフトウェアの公開鍵 E で暗号化(署名検証)をして、 rK を得る(S61)。この乱数 r の項を除去することが出来るのは、証明データ検証装置10のみである。 r の項を除去し、 K を得る(S62)。実行制御手段120は、この得られた K の値をもって、利用を制限されたソフトウェア100を復号化して、実行をおこなう(S63)。

【0042】以上説明したように、利用制限をされたソフトウェアに対する証明用補助情報としてのライセンスチケットをつかって、ユーザのアクセス資格を検証することにより、ソフトウェアの実行を可能にすることができる。ライセンスチケットの発行を管理することにより、ソフトウェアプロバイダへの正しい利用料(ライセ

ンスフィー)を支払うことが可能になる。また第二の実施例で説明したように、ライセンスチケットの発行を予め定められたライセンス数の上限まで発行する管理をすることも可能になる。もちろん、これらの認証動作は全てローカルな環境で実行されるので、ソフトウェア利用時にオンラインである必要が全くない。

【0043】本発明によるソフトウェアは利用制限がかかっており、それ単体では動作は不可能なので、CD-ROMにいて配布したり、インターネット上のWWWサーバやFTPサーバなどに置くことが可能である。利用したいユーザはライセンスチケットを購入してソフトウェアの利用制限を解除して使用することができる。ライセンスチケットの有効期間を短くすることにより、一ライセンスチケットの発行に対しての代金を安く設定して、安く多量に販売するというライセンス形態も可能になる。

【0044】なお、本発明は上述の実施例に限定されるものではなく、種々変更が可能である。例えば、アクセス資格認証にRSA公開鍵暗号系の手法を使用したか、他の暗号系も適用可能である。

【0045】

【発明の効果】以上説明したように、本発明によれば、ソフトウェアの二次使用による不正使用をオンラインでも、オフラインでも防止することが可能になり、正当なライセンス管理システムを構築できる。

【図面の簡単な説明】

【図1】 本発明の実施例のライセンス管理装置の概略を示すブロック図である。

【図2】 上述実施例の変形例を示すブロック図である。

【図3】 上述実施例のソフトウェアの暗号化の一例を示す図である。

【図4】 上述実施例の認証用データの生成方法の一例を示す図である。

【図5】 上述実施例のライセンスチケット発行装置の一例を示す図である。

【図6】 上述実施例のユーザ情報データベースの一例を示す図である。

【図7】 上述実施例のソフトウェア情報データベースの一例を示す図である。

【図8】 上述実施例のライセンスチケットの生成方法の一例を示す図である。

【図9】 上述実施例のソフトウェア情報データベースの別の例を示す図である。

【図10】 上述実施例のライセンスチケットの生成方法の別の例を示す図である。

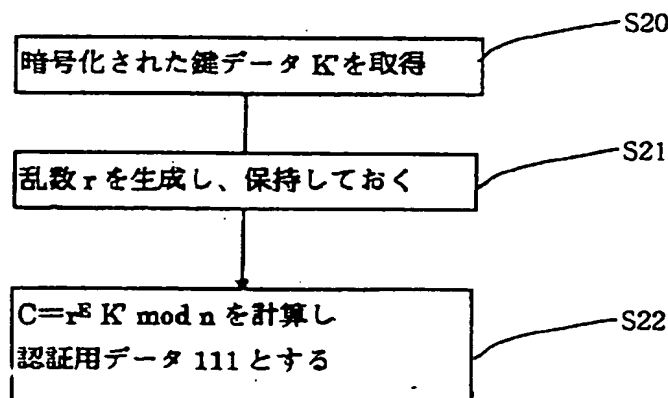
【図11】 上述実施例の証明データ生成方法の一例を示す図である。

【図12】 上述実施例の証明データ認証手段と実行制御手段の動作を示す図である。

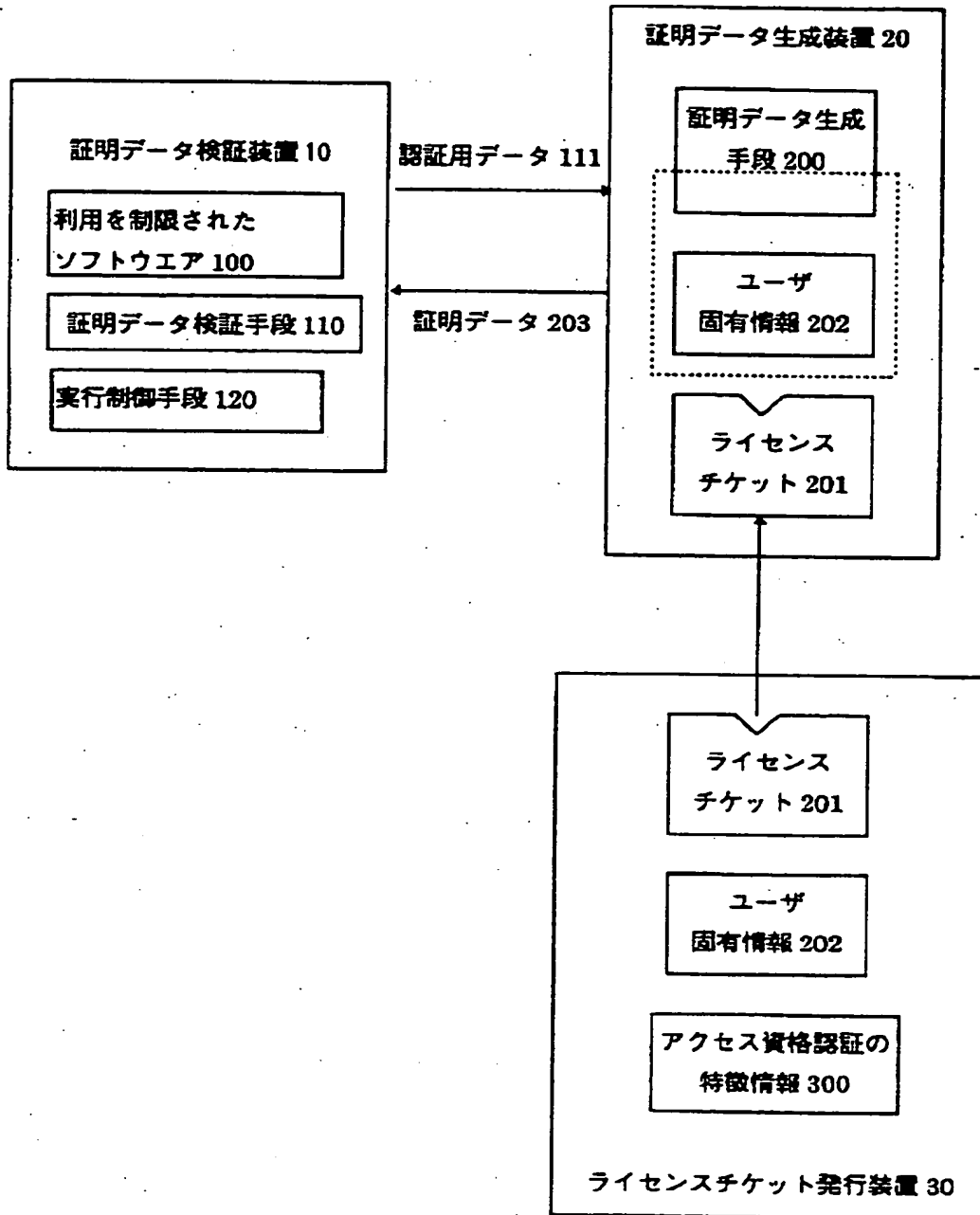
【符号の説明】

- 10 証明データ検証装置
- 20 証明データ生成装置
- 30 アクセスチケット生成装置
- 100 利用を制限されたソフトウェア
- 110 証明データ検証手段
- 120 実行制御手段
- 200 証明データ生成手段
- 201 ライセンスチケット
- 202 ユーザ固有情報
- 300 アクセス資格認証の特徴情報
- 301 ライセンスチケット生成手段
- 302 ユーザ情報管理手段
- 303 ソフトウェア情報管理手段
- 304 ライセンス数管理手段
- 310 ユーザ情報データベース
- 320 ソフトウェア情報データベース

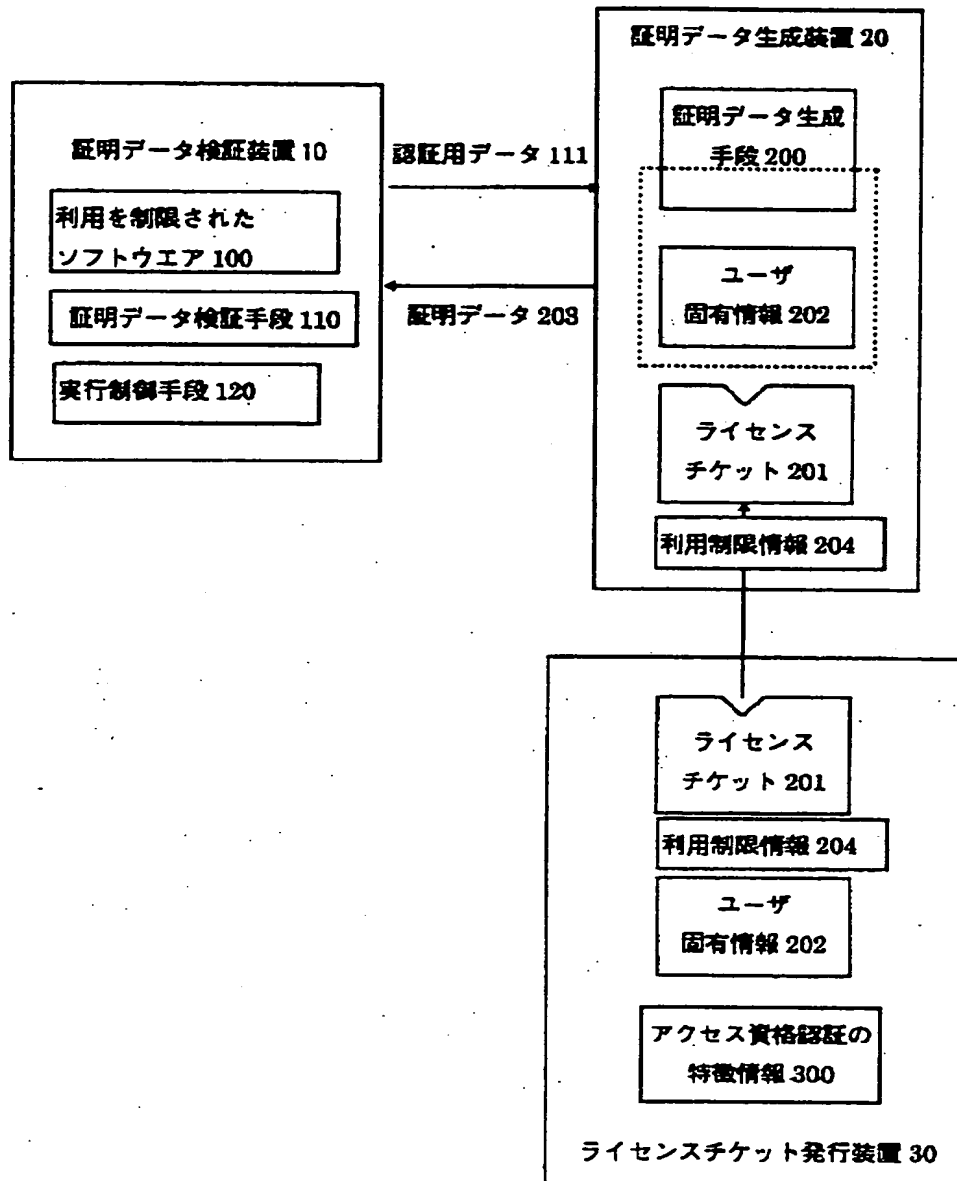
【図4】



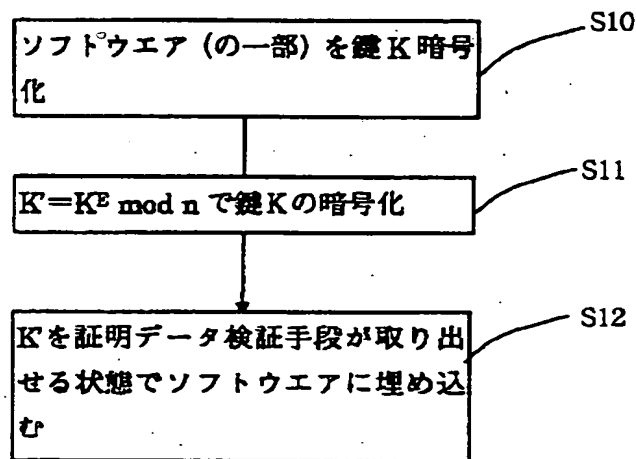
【図1】



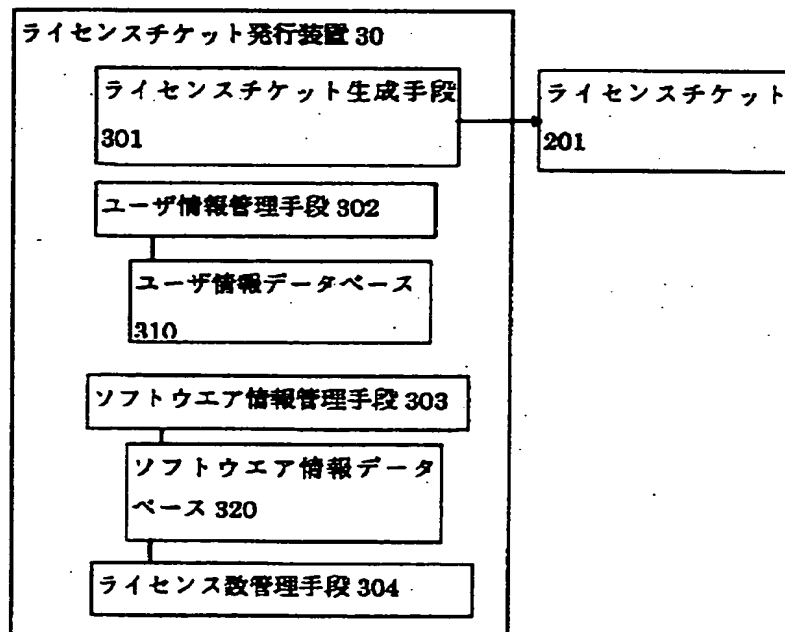
【図 2】



【図3】



【図5】



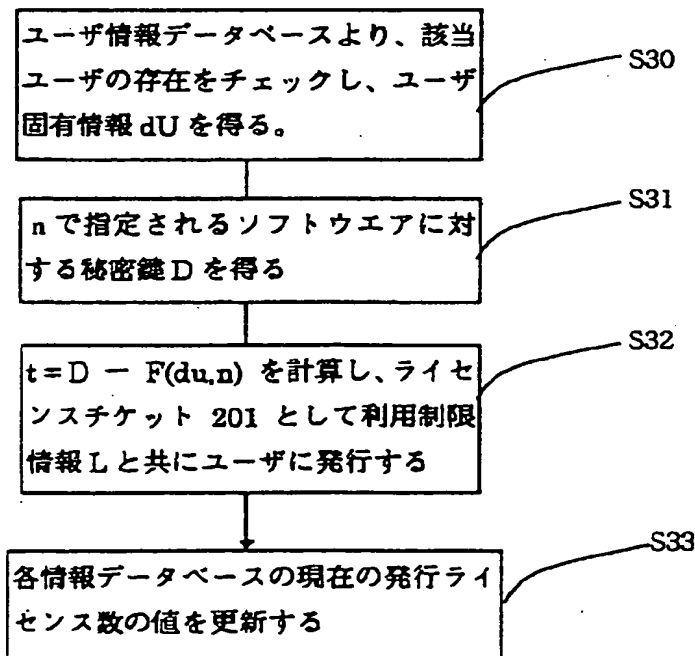
【図6】

ユーザ ID	ユーザ名 U	ユーザ固有情報 dU	チケット数	ライセンスチケットリスト
16047	s.kojima	1239042....	4	
17440	j.nakagaki	6756923...	7	

【図 7】

Software ID	Software 名	公開情報 (n)	秘密情報 (D)	発行チケット数	ライセンスチケットリスト
10001	Gloval View	3849214...	34355.....	33	
10002	Docu Works	6432876...	61321....	19	

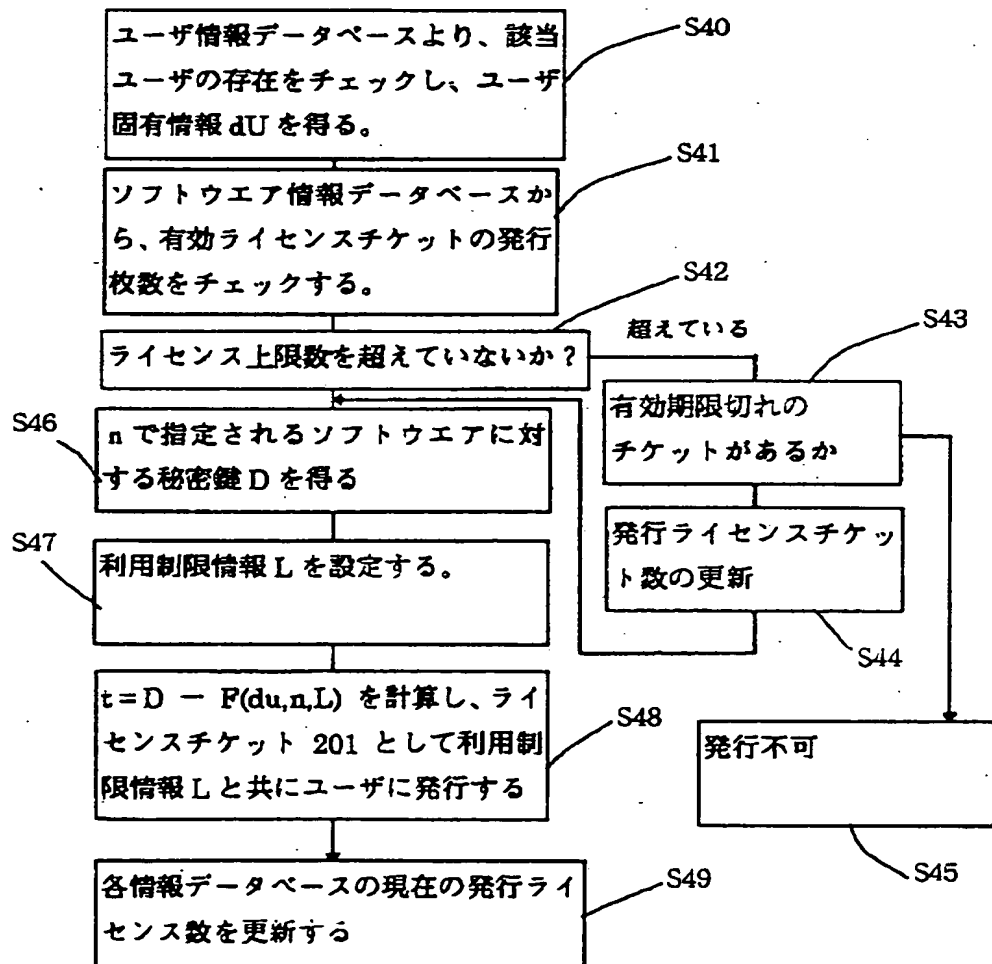
【図 8】



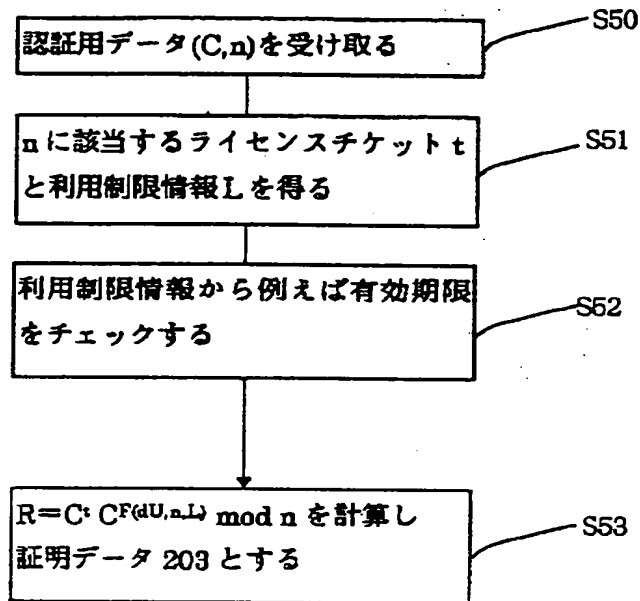
【図 9】

Software ID	Software 名	公開情報 (n)	秘密情報 (D)	設定ライセンス数	有効チケット数	ライセンスチケットリスト
10001	Gloval View	3849214..	34355.....	50	39	
10002	Docu Works	6432876..	61321....	20	19	

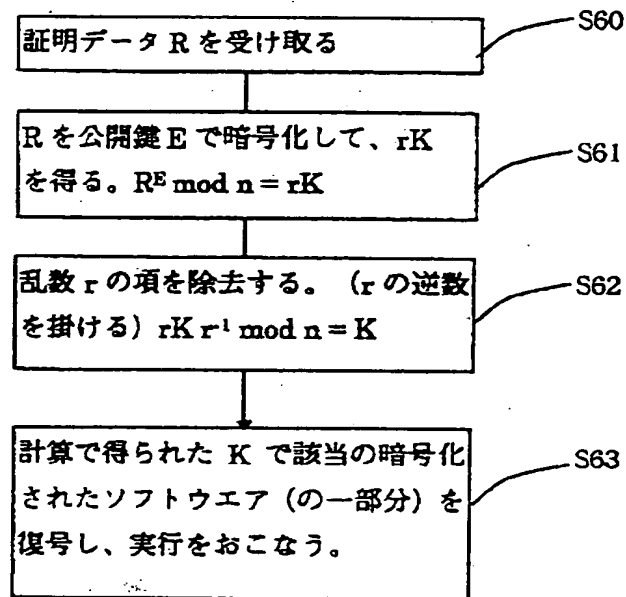
【図 10】



【図 11】



【図 12】



フロントページの続き

(51)Int.Cl.⁶

G 0 9 C 1/00
H 0 4 L 9/32

識別記号
6 4 0

F I

G 0 9 C 1/00
H 0 4 L 9/00

6 4 0 E
6 7 5 B